IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

DONNA BLUE, *individually, and on behalf of those similarly situated,*	Case No. 5:24-cv-706
Plaintiff,	
v.	**COMPLAINT - CLASS ACTION**
CUMBERLAND COUNTY HOSPITAL SYSTEM, INC. d/b/a CAPE FEAR VALLEY HEALTH SYSTEM,	**JURY TRIAL DEMANDED**
Defendant.	

Plaintiff Donna Blue ("Plaintiff"), individually and on behalf of herself and all others similarly situated, by and through her attorneys of record, asserts the following against Defendant Cumberland County Hospital System. Inc. d/b/a Cape Fear Valley Health System ("Cape Fear" or "Defendant").

INTRODUCTION

1. This class action lawsuit arises out of Cape Fear's unlawful use of third-party tracking technologies by data brokers such as Meta and Google LLC (the "Tracking Tools") to surreptitiously intercept and disclose its patients' private and protected communications, including communications concerning highly sensitive personal health information, to third parties without patients' knowledge or consent.

2. By purposely embedding and deploying the Tracking Tools on Cape Fear's web properties, Cape Fear engages in the unauthorized disclosure of its patients' highly sensitive Protected Health Information ("PHI") and Personally Identifiable Information ("PII") to third

parties including, but not limited to, Meta Platforms, Inc. d/b/a/ Meta ("Facebook") and Google LLC ("Google").[1] Such disclosures of PHI and PII violate state and federal law.

3. Cape Fear is North Carolina's eighth largest health system, with eight hospitals within the system.[2] Cape Fear has over 7,500 employees and over 1,000 physicians.[3]

4. Cape Fear encourages patients and prospective patients to use its website, available at https://www.capefearvalley.com/home/index.aspx (the "Website") and its MyChart patient portal, available at https://www.capefearvalley.com/mychart/ (the "Portal"), to communicate about symptoms and conditions, research treatments, lookup physicians, schedule appointments, pay their bills, among other activities.[4]

5. Unbeknownst to its patients and prospective patients, their communications were intercepted and disclosed to third parties through Cape Fear's use of Tracking Tools, third party trackers from companies including Facebook and Google.

6. One of the Tracking Tools Cape Fear deployed on its Website is the Meta Pixel ("Pixel").[5] The Pixel is a snippet of code that, when embedded on a website, tracks the website visitor's activity on that website and sends that data to a third party, like Meta.

---

[1] While this complaint focuses on tracking tools from Facebook and Google, research shows that Defendant also embedded tracking codes from a number of other marketing companies including Doubleclick and LinkedIn, which are also capable of collecting personal health information and linking it to a specific individual.

[2] Cape Fear's "About Us" page, https://www.capefearvalley.com/about/index.html.

[3] See https://www.linkedin.com/company/cape-fear-valley-health.

[4] Without the benefit of discovery, Plaintiff does not have the evidence that Cape Fear currently installs third-party trackers on its Patient Portal; however, given that Defendant did choose to embed third-party tracking codes on the bill pay webpage, upon information and good faith belief Plaintiff alleges that Cape Fear installed such trackers in the Portal as well.

[5] Meta also provides other tracking technologies that give the same or similar tracking functionalities as the Pixel including, but not limited to, Conversions API, SDKs, and Audiences.

7. The Pixel tracks and logs the pages a website user visits during a website session that reveals their patient status and other PII and PHI, searches, and other submissions to the website. Indeed, the Pixel is routinely used to target specific individuals by utilizing the data gathered through the Pixel to build profiles for the purpose of future targeting and marketing.

8. The information Cape Fear transmitted to third parties, such as Meta, without Plaintiff's consent included PHI,[6] which is some of the most personal and sensitive data Plaintiff has.

9. Additionally, when a patient communicates with Cape Fear's Web Properties where the Pixel is present, Pixel source code causes the exact content of the patients' communications with the Website to be re-directed to Meta in a way that identifies the person as a patient.

10. Here, Plaintiff used the Website to communicate about her sensitive health conditions and symptoms, research potential treatments and physicians, and make appointments. Unbeknownst to Plaintiff, when she communicated about her PHI, the Pixel secretly intercepted, recorded, and transmitted those private communications to Meta along with unique identifiers Meta could use to identify Plaintiff.

Absent discovery, Plaintiff is unable to independently confirm whether Defendant installed such tracking technologies on its Website.

[6] Under HIPAA, "health information" is defined as "any information[], whether oral or recorded in any form or medium, that . . . [i]s created or received by a health care provider . . . and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Additionally, HIPAA defines "health care" as "care, services, or supplies related to the health of an individual" and includes, but is not limited to, the "[s]ale or dispensing of drug, device, equipment, or other item in accordance with a prescription." *Id.*

11. As a result of Defendant's use of the Pixel, Plaintiff's and Class Members' PHI and PII including, but not limited to, computer IP addresses, patient status, health conditions and symptoms, treatments, physicians, appointment details, and unique personal identifiers used to link the sensitive web communications to Plaintiff and Class Members, were compromised and disclosed to third parties such as Meta without authorization or consent.

12. Such private information allows Meta to know that a specific patient was seeking confidential health care or exploring treatment for a specific condition.

13. Defendant's Tracking Tools have also transmitted patients' PHI and PII to additional unauthorized third parties for marketing and advertising purposes, including Google.

14. Google's tracking technologies operate much like the Meta Pixel. As one District Court recently described:

> Whenever a user visits a website that is running Google Analytics, Ad Manager, or some similar Google service, Google's software directs the user's browser to send a separate communication to Google. This happens even when users are in private browsing mode, unbeknownst to website developers or the users themselves. The operation is not in dispute. When a user visits a website, the user's browser sends a "GET" request to the website to retrieve it. This GET request contains the following information: the Request URL, or the URL of the specific webpage the user is trying to access; the user's IP address; the User-agent, which identifies the user's device platform and browser; user's geolocation, if available; the Referer, which is the URL of the page on which the user clicked a link to access a new page; event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and the actual search queries on the site. At the same time, the user's browser reads Google's code, which is embedded on the website. Google's code instructs the user's browser to send a second and concurrent transmission directly to Google. This second transmission tells Google exactly what a user's browser communicated to the website.[7]

[7] *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at *2 (N.D. Cal. Aug. 7, 2023). As explained by the Court in *Brown*, Google connects user data to IP addresses; IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifiable information that constitutes one of the 18 HIPAA identifiers of PHI. *See* 45 C.F.R. § 164.514 (2).

15. In secretly deploying the Tracking Tools on its Website to intercept and disclose website communications concerning its patients' and prospective patients' PHI and PII, Defendant acted with a tortious and criminal purpose in violation of state and federal laws.

16. Plaintiff and Class Members never consented to, authorized, or otherwise agreed to allow Defendant to disclose their PHI and PII to anyone other than those reasonably believed to be part of Cape Fear, acting in some healthcare-related capacity. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's and Class Members' PHI and PII to Meta, Google, and other third parties.

17. Given the nature of Meta and Google's businesses as two of the world's largest online advertising companies, Plaintiff's and Class Members' PHI and PII can and will likely be further used by or exposed to additional third parties.

18. As a direct and proximate result of Defendant's unauthorized exposure of Plaintiff's and Class Members' PHI and PII, Plaintiff and Class Members have suffered injury, including an invasion of privacy, loss of the benefit of the bargain Plaintiff and Class Members considered at the time they bargained for healthcare services and agreed to use Defendant's Website for services, statutory damages, and the continued and ongoing risk to their PHI and PII.

19. Plaintiff brings this action individually, and on behalf of a Class of similarly situated individuals, to recover for harms suffered and assert the following claims: (i) Violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511; (ii) Negligence; (iii) Breach of Express Contract; (iv) Breach of Implied Duty of Good Faith and Fair Dealing; (v) Breach of Implied Contract; (vi) Breach of Fiduciary Duty and (vii) Unjust Enrichment.

PARTIES

20. Plaintiff Donna Blue is, and at all relevant times was, an individual residing in Fayetteville, Cumberland County, in the State of North Carolina.

21. Defendant Cumberland County Hospital System. Inc. d/b/a Cape Fear Valley Health System, is a North Carolina corporation, headquartered at 1638 Owen Drive, Fayetteville, NC 28304.

22. Defendant operates numerous hospitals and urgent care centers throughout the state of North Carolina under the name Cape Fear Valley Health.

23. Cape Fear Valley Health is a health care provider and is a covered entity under HIPAA.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under federal law, including ECPA, 18 U.S.C. § 2511, *et seq*.

25. This Court has supplemental jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1367.

26. This Court has personal jurisdiction over Defendant because Cape Fear is a North Carolina corporation with its principal place of business in this District.

27. Venue is proper under 28 U.S.C. §§ 1391(b)(1)-(2) because Defendant's principal place of business is in this District and a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Federal Regulators Have Warned Healthcare Providers About the Impermissible Use of Tracking Technologies.

28. The surreptitious collection and disclosure of PHI and PII is a serious data security and privacy issue. Both the Federal Trade Commission ("FTC") and HHS have reiterated the necessity for data security and privacy concerning health information.

29. The FTC published a bulletin entitled *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, in which it noted that "[h]ealth information is not just about medications, procedures, and diagnoses. Rather, it is anything that conveys information—or enables an inference—about a consumer's health. Indeed, [recent FTC enforcement actions involving] Premom, BetterHelp, GoodRx and Flo Health make clear that the fact that a consumer is using a particular health-related app or website—one related to mental health or fertility, for example—or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information."[8]

30. The FTC informs companies that provide healthcare services that they should not use tracking technologies to collect sensitive health information and disclose it to various platforms without informed consent:

> **Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.** In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps,

[8] *See* Elisa Jillison, *Protecting the privacy of health information: A Baker's dozen takeaways from FTC cases*, the FTC Business Blog (July 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

> watch out. [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.[9]

31. HHS affirmed that HIPAA and its regulations prohibit the transmission of individually identifiable health information ("IIHI") by tracking stechnology like the Google and Meta without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[10]

32. In July 2023, the FTC and HHS sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of PHI to third parties.[11] The letter highlighted the "risks and concerns about the use of technologies, such as the Meta/Facebook Pixel and Google Analytics, that can

---

[9] *Id.* (emphasis added).

[10] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (noting that "IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."). This guidance was recently vacated in part due to the court finding it in part to be the product of improper rulemaking, and it is cited for reference only until OCR updates its guidance, should it do so in the future. *See American Hosp. Ass'n. v. Becerra*, 2024 WL 3075865 (S.D. Tex., Jun. 20, 2024). The Court's Order found only that OCR's guidance regarding covered entities' collection and disclosure to third parties of users' IP addresses while they navigated unauthenticated public webpages ("UPWs") was improper rulemaking. The Order in no way affects or undermines OCR's guidance regarding covered entities disclosing unique personal identifiers, such as Google or Facebook identifiers, to third parties while patients make appointments for particular conditions, pay medical bills or log into (or use) a patient portal. *See id.* at 3-4, 31, n. 8 (vacating OCR guidance with respect to the "Proscribed Combination" defined as "circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW addressing specific health conditions or healthcare providers" but stating that "[s]uch vacatur is not intended to, and should not be construed as, limiting the legal operability of other guidance in the germane HHS document.").

[11] https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information

track a user's online activities," and warned about "[i]mpermissible disclosures of an individual's personal health information to third parties" that could "result in a wide range of harms to an individual or others."[12] According to the letter, "[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."[13]

33. Despite these clear warnings from federal regulators, Defendant Cape Fear embedded Tracking Tools on its Website to secretly track its patients' communications regarding healthcare information and disclose those communications to third parties.

B. The Meta Pixel

34. Through its Web Properties, Defendant connects Plaintiff and Class Members to Defendant's digital health care platforms with a core goal of increasing profitability.

35. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely embedded and deployed the Meta Pixel on its Website and, upon information and good faith belief, its Portal.[14] By doing so, Defendant surreptitiously shared its

[12] https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

[13] *Id.*

[14] At the time of filing this Complaint, Plaintiff is unable to determine whether Pixels or other third-party tracking tools were embedded inside Defendant's MyChart Portal. Given Defendant's use of the Meta Pixel and Google trackers on other pages of the Website *including the log-in and sign-up pages for its patient Portal, as well as the bill pay portion of the website*, Plaintiff reasonably believes and, therefore, avers that Defendant used the Pixels and other Tracking Tools to track information on its entire digital platform, including inside its MyChart Portal. *See also* Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022) (listing examples of hospitals that used third party trackers inside password-protected patient portals), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

patients' and prospective patients' identities and online activity including private communications and search results related to conditions, symptoms, treatments, and physicians with Meta.

36. Meta's core business function is to sell advertising, and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual revenue comes from advertising—a practice in which Meta actively participates by using algorithms that approve and deny ads based on the ads' content, human moderators that further review ads for both legality and aesthetics prior to and after the ads are published, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

37. Over the last decade, Meta has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

38. Meta's advertising business has been successful due, in significant part, to Meta's ability to target users, both based on information users provide to Meta, and based on other information about users Meta extracts from the Internet at large. Given the highly specific data used to target particular users, thousands of companies and individuals utilize Facebook's advertising services.

39. One of Meta's most powerful advertising tools is the Meta Pixel, which it first launched as the Facebook Pixel in 2015.

40. The Pixel was branded as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." Meta stated:

> Facebook pixel, [is] a new way to report and optimize for conversions, build audiences[,] and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.

> Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous blog post (Announcing Upgrades to Conversion Tracking and Optimization at Facebook) are supported through Facebook pixel as well.
>
> [Advertisers and website operators] can use Facebook pixel to track and optimize for conversions by adding standard events (*e.g.*, Purchase) to your Facebook pixel base code on appropriate pages (*e.g.*, purchase confirmation page).[15]

41. The Pixel is an easily attainable piece of code that Meta makes available to website developers for free. In exchange, at a minimum, website developers must agree to Meta's Business Tool Terms.[16]

42. The Business Tools Terms note that the Meta's Business Tools including the Pixel capture two types of information: "Contact Information" which "personally identifies individuals," and "Event Data" which contains additional information about people and their use of a developer's website.[17]

43. The Business Tools Terms also require websites to "provide[] robust and sufficiently prominent notice to users . . . on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Meta, may . . . collect or receive information from your websites and elsewhere on the Internet and use that information to . . . deliver ads, (b)

---

[15] Cecile Ho, *Announcing Facebook Pixel*, Meta (Oct. 14, 2015), https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/.

[16] *See* Meta Business Tool Terms, https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr ("When you use any of the Meta Business Tools . . . or otherwise enable the collection of Business Tool Data . . . these Business Tool Terms govern the use of that data").

[17] *Id.*, § 1(a)(i)-(ii).

how users can opt out of the collection and use of information . . . and (c) where a user can access a mechanism for exercising such choice[.]"[18]

44. Even with these protocols in place, Meta prohibits the disclosure of Business Tools Data "that you know or reasonably should know . . . includes health, financial information or other categories of sensitive information (including any information defined as sensitive under applicable laws, regulations and applicable industry guidelines)."[19]

45. After agreeing to the Business Tools Terms, website developers can choose to install and use the Pixel on their websites to track and measure certain actions, such as a website visitor's text searches and page views, including the detailed URLs triggered by page views. When a website visitor takes an action a developer chooses to track on its website, the Pixel is triggered and sends data about that "Event" to Meta. All of this happens without the user's knowledge or consent.

46. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the Internet. Each "client device" (such as a computer, tablet, or smart phone) accesses web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

47. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

---

[18] *Id.*, § 3(c)(i).

[19] *Id.*, § 1(h).

48. A browsing session online may consist of thousands of web communications. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- An **HTTP Request** is an electronic communication a website visitor sends from his device's browser to the website's server. There are two types of HTTP Requests: (1) GET Requests, which are one of the most common types of HTTP Requests—in addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies; and (2) POST Requests which can send a large amount of data outside of the URL. In this case, a patient's HTTP Request would be asking Defendant's Website to get certain information, such as a list of clinic locations or prescriptions. So that servers can better understand what information users are requesting, HTTP Requests also use URLs that contain parameters, which use variables and assigned values in the URL to pass additional information through the HTTP Request.

- **Cookies** are a text file that website operators and others use to store information on the website visitor's device; these can later be communicated to a server or servers. Cookies are sent with HTTP Requests from website visitor's devices to the host server. Some cookies are "third-party cookies," which means they can store and communicate data when visiting one website to an entirely different website. Third-party cookies are created by a website with a domain name other than the one the user is visiting, in this case Meta.[20] There are also "first-party cookies," like the fbp cookie, which is created by the website the user is visiting, in this case Defendant.[21] Meta uses both first- and third-party cookies in Pixel to link Facebook IDs and Facebook profiles, and Defendant sends these identifiers to Meta.

- An **HTTP Response** is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the website visitor's device's web browser from the host server. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data. The HTTP Response is when the website sends the requested information (*see* the HTTP Request); this is sometimes called the "Markup."

---

[20] *Third-Party Cookie*, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable using web developer tools to inspect a website's cookies and track network activity.

[21] *First-Party Cookie*, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable using web developer tools to inspect a website's cookies and track network activity.

49. A user's HTTP Request asks Defendant's Website to retrieve certain information (such as "Orthopedics"). The HTTP Response then renders or loads the requested information in the form of Markup (i.e., the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Website).

50. Every website, including Defendant's, is composed of Markup and "Source Code."

51. Source code is a set of instructions that commands the website visitor's browser to take certain actions when the web page loads or when a specified event triggers the code.

52. Source code may also command a web browser to transmit data to third parties in the form of an HTTP Request. Such data transmissions allow a website to export data about users and their actions to third parties. Third parties receiving this data are typically configured to track user data and communications for marketing purposes.

53. Transmission of such data occurs in the background without notifying the web browser's user. The pixels are invisible to website users and thus, without any knowledge, authorization, or action by the user, the website site developer (or website commander) can use its source code to contemporaneously and invisibly re-direct the user's PII and PHI to third parties. Through the Pixel, Defendant uses source code that can accomplish just that.

54. The Pixel "tracks the people and the types of actions they take."[22] According to Meta, the Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by understanding the actions [website visitors] take on [its] website."[23] Thus, by

[22] *Retargeting*, Facebook, https://www.facebook.com/business/goals/retargeting.

[23] *About Meta Pixel*, Meta Business Help Center, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

secretly recording and transmitting data to Meta—without the user's knowledge or consent—the Pixel acts much like a traditional wiretap controlled by Defendant.

55. Through this online tracking technology, Meta intercepts each page a user visits, what buttons they click, as well as the specific information the user inputs into the website and other searches conducted. The Pixel sends each of these pieces of information to Meta with PII, such as the user's IP address. Meta stores this data on its own servers, in some instances for years on end, and independently uses the data for its own financial gain.

56. For example, when a patient visits https://www.capefearvalley.com/ and selects "Cancer," the patient's browser automatically sends an HTTP Request to Defendant's web server. Defendant's web server automatically returns an HTTP Response, which loads the Markup for that particular webpage. As depicted below, the user only sees the Markup, not Defendant's source code or underlying HTTP Requests and Responses.

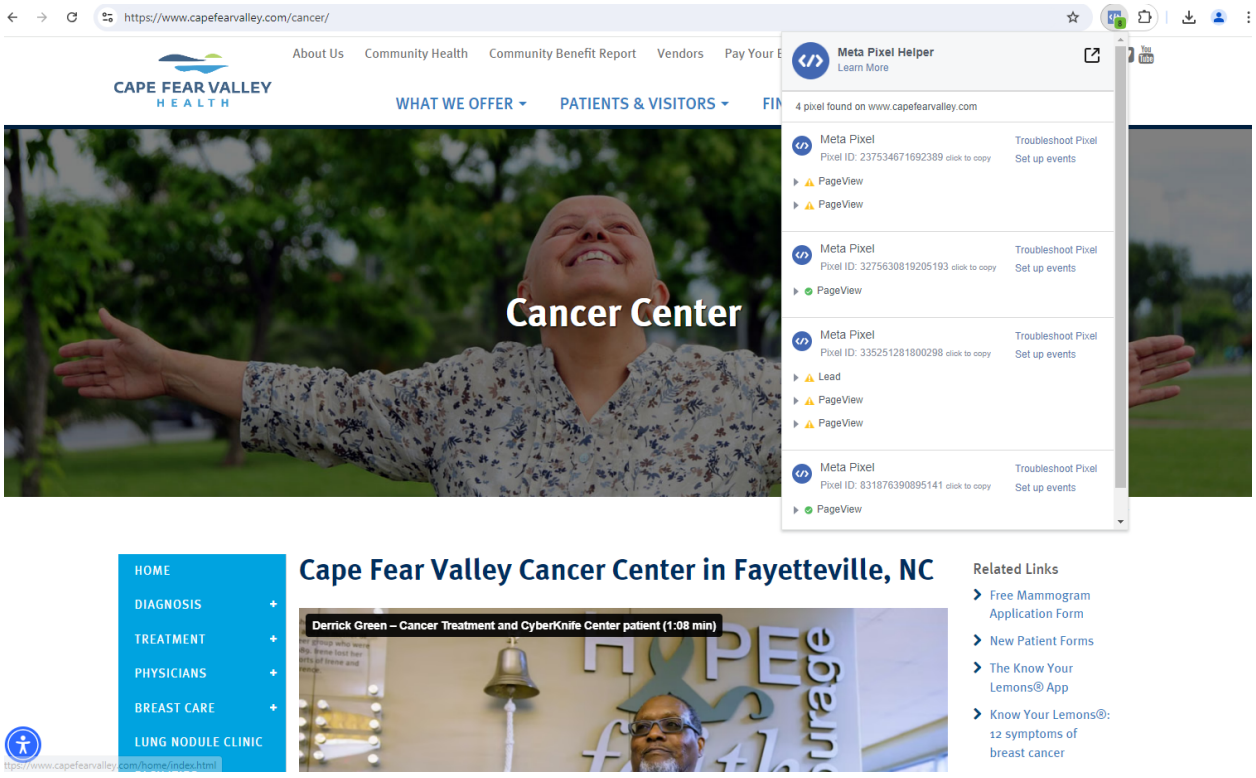


Figure 1: The image above is a screenshot taken from the user's web browser upon visiting https://www.capefearvalley.com/cancer/

57. The image above displays the Markup of Defendant's webpage. Behind the scenes, however, Tracking Technologies like the Meta Pixel and Google Analytics are embedded in the source code, automatically transmitting everything the patient does on the webpage and effectively opening a hidden spy window into the patients' browser.

58. This data is often associated with the individual user's Facebook account. For example, if the user is logged into their Facebook account (or has been logged in recently) when the user visits Defendant's website, Meta receives third-party cookies allowing Meta to link the data collected by the Pixel to the specific Facebook user. In other words, a user's personal and private information sent by the Meta Pixel to Facebook is sent alongside that user's personal identifiers, including IP address and cookie values, which can be linked to the user's unique Facebook account.

59. Meta accomplishes this by placing cookies in the web browsers of users logged into their services, which aids Meta in identifying users.

60. One such example is the "c_user" cookie, which is a third-party cookie assigned to each person with a Facebook account. The "c_user" cookie contains a numerical value known as the Facebook ID that uniquely identifies a Facebook user. It is composed of a unique and persistent set of numbers.

61. A user's Facebook ID is linked to their Facebook profile, which contains a wide range of demographic and other information about the user including pictures, personal interests, work history, relationship status, and other details.

62. Because a user's Facebook ID uniquely identifies their Facebook account, Meta—or any ordinary person—can use the Facebook ID to locate, access, and view the user's corresponding Facebook profile. Thus, when a Facebook user visits Defendant's Website while logged in to their Facebook account, the Pixel transmits the user's private web communications with Defendant along with the "c_user" cookie. Meta can then use this information to match the web communications with the user's Facebook ID.

63. Even if a user does not have a Facebook account or is not logged in to Facebook when browsing Defendant's Website, the Pixel transmits the user's web communications with Defendant's Website to Meta along with a unique identifier associated with another cookie called the "_fbp" cookie. Meta can then use that unique identifier to link the user's web communications with the user's Facebook ID. And if a user who does not have a Facebook account later creates an account, Meta may be able to associate the user's historical browsing history intercepted via the Pixel and "_fbp" cookie to the newly created account.

64. Meta's Business Tools Terms make clear that the Pixel is meant to "match the Contact Information" of users "against user IDs . . . as well as to combine those user IDs with corresponding Event Data."[24]

65. After Meta processes users' intercepted information, it makes the relevant analytics available to Cape Fear through Meta's Event Manager tool.

[24] *Meta Business Tool Terms, Section 2(a)(i)(1),* https://www.facebook.com/legal/businesstech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr.

66. Using the Events Manager, Cape Fear can review a summary of users' activity including the pages, parameters, and URLs sent through the Pixel,[25] as well as any included metadata.[26]

67. Without any knowledge, authorization, or action by a user, a website owner like Defendant can use its Source Code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to Meta. Meta then uses this information to match the user with their Facebook ID.

68. Judge William H. Orrick on the United States District Court for the Northern District of California summarized how this process plays out:

> To understand how the Meta Pixel typically works, imagine the following scenario. A shoe company wishes to gather certain information on customers and potential customers who visit its website. The shoe company first agrees to Meta's Business Tools Terms (discussed below), which govern the use of data from the Pixel. The shoe company then customizes the Meta Pixel to track, say, every time a site visitor clicks on the "sale" button on its website, which is called an "Event." Every time a user accesses the website and clicks on the "sale" button (i.e., an "Event" occurs), it triggers the Meta Pixel, which then sends certain data to Meta. Meta will attempt to match the customer data that it receives to Meta users—Meta cannot match non-Meta users. The shoe company may then choose to create "Custom Audiences" (i.e., all of the customers and potential customers who clicked on the "sale" button) who will receive targeted ads on Facebook, Instagram, and publishers within Meta's Audience Network. Meta may also provide the shoe company with de-identified, aggregated information so the shoe company understands the impact of its ads by measuring what happens when people see them. Meta does not reveal the identity

[25] *How to view pages, parameters and URLs in Meta Events Manager*, https://www.facebook.com/business/help/815029860145251 ("In Meta Events Manager, you can see a summary of pages, parameters and URLs recently sent through the Meta Pixel . . . .").

[26] A web developer using the Events Manager can "[c]lick on the filter icon to select what activity types and details are display." Developers can sort by activity types, including "automatically logged pixel events," which may contain metadata. *Test your app or web browser events using the test events tool*, https://www.facebook.com/business/help/2040882565969969?id=1205376682832142.

of the matched Meta users to the shoe company.[27]

69. The Pixel also allows a healthcare company, like Defendant, to impact the delivery of ads, measure cross-device conversions, create custom audiences, and save money on advertising and marketing costs.[28] But, most relevant here, the Pixel allowed Defendant and Meta to track users secretly on Defendant's Web Properties and intercept their communications with Defendant.

70. When visitors to Defendant's Web Properties, like Plaintiff and Class Members, communicated with Defendant or inquired about personal health-related topics, that information was transmitted to and intercepted by Meta.

71. The PHI intercepted, recorded, and transmitted to Meta includes, but is not limited to, exact search terms and search results, patient status, health symptoms, health conditions, treatments, appointment details, and physicians and locations sought.

72. During that same transmission, Defendant would also provide Meta with the patient's PII, such as their Facebook ID number, persistent cookies, device ID, and computer IP addresses. This information makes it easy to link private communications with Defendant via the Web Properties to a specific and identifiable Facebook user.

73. Once Meta has that data, it processes, analyzes, and assimilates it into databases like Core Audiences or Custom Audiences for advertising purposes. If the website visitor is also a Facebook user, Meta will associate the information that it collects from the visitor with a Facebook ID that identifies the user's name and Facebook profile.

---

[27] *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *2 (N.D. Cal. Dec. 22, 2022) (internal citations omitted). In describing Pixel technology in *In re Meta Pixel Healthcare Litigation*, the court referenced the declaration of expert Richard M. Smith, which details the manner in which the challenged Pixel technology works and Meta's arrangements with health providers that employ it. *See* Declaration of Richard M. Smith, *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO (N.D. Cal.) [ECF 49].

[28] *Meta Pixel*, https://www.facebook.com/business/tools/meta-pixel?ref=search_new_2.

74. In sum, the Pixel allows Meta to learn, manipulate, and use for financial gain, the medical and private content Defendant's Web Properties visitors communicated, viewed, or otherwise interacted with on Defendant's Web Properties.

C. Google Tracking Code.

75. Like the Meta Pixel, Google creates code that website developers can install on their websites to track user activity. Whenever a user visits a website that is running Google tracking code, Google's code directs the user's browser to send a separate and concurrent communication to Google without the user's knowledge.

76. The information that is intercepted and transmitted to Google via the Google tracking code includes: (i) the URL of the specific webpage a user is trying to access; (ii) the user's IP address; (iii) the User-agent, which identifies the user's device platform and browser; (iv) the user's geolocation, if available; (v) the Referer, which is the URL of the page on which the user clicked a link to access a new page; (vi) event data, which describes how users interact with a website, for example, whether they saw an ad or played a video; and (vii) actual search queries on the site.

77. Google tracking code tells Google exactly what a user's browser communicated to the website.

78. Like with the Meta Pixel, the user's communications to the website are transmitted to Google together with cookies and other unique identifiers that Google can use to match the communications to individuals who use Google's services.

79. Information sent to Google is sent alongside the users' unique identifier ("_ga" or "CID" cookies), thereby allowing individual patients' communications with Cape Fear, and the

PHI and PII contained in those communications, to be linked to their unique Google accounts and therefore their identity.[29]

80. Google logs a user's browsing activities on non-Google websites and uses this data for serving personalized ads.

D. Cape Fear Deploys Third-Party Tracking Tools to Intercept and Disclose PHI and PII.

81. As an example of how the Meta Pixel operated on Cape Fear's Website, consider a visitor who goes to the Website and uses the search bar to search for "cancer."

82. The search result takes the visitor to the https://www.CapeFear.org/search?q=cancer webpage. When doing so, the visitor's browser sends a GET Request to Defendant's server, requesting that server to load the webpage.

83. At the same time, the Pixel causes the visitor's browser to secretly intercept and record the visitor's communication with Cape Fear's Website including the specific URL requested and transmit the private communication to Meta with unique identifiers used to link the communication to a specific Facebook user.

84. The "dl" path shows the specific URL for the page requested by the visitor's browser, including the substantive description and disclosure of the visitor's search for "cancer." This transmission, as explained herein, also contains the Pixel's transmission of the _fbp cookie, the c_user cookie (the Facebook ID), and other cookies and identifiers used to identify the website visitor by name and Facebook account. Thus, the fact that a patient or prospective patient is using or considering using Cape Fear for healthcare services related to cancer is transmitted to Meta.

[29] *See Brown v. Google LLC*, 2023 WL 5029899, at fn. 6, *supra*, note 7 (quoting Google employee deposition testimony explaining how Google tracks user data).

Disclosure of that information reveals to Meta the website visitor's status as a patient or prospective patient with Cape Fear, seeking services or treatment for cancer.

85. If that same patient inquired about specific cancer treatment center or a provider specializing in cancer, the Pixel would likewise intercept those communications and transmit them to Meta along with the patient's unique identifiers, as reflected in ***Figures 2-4*** below:

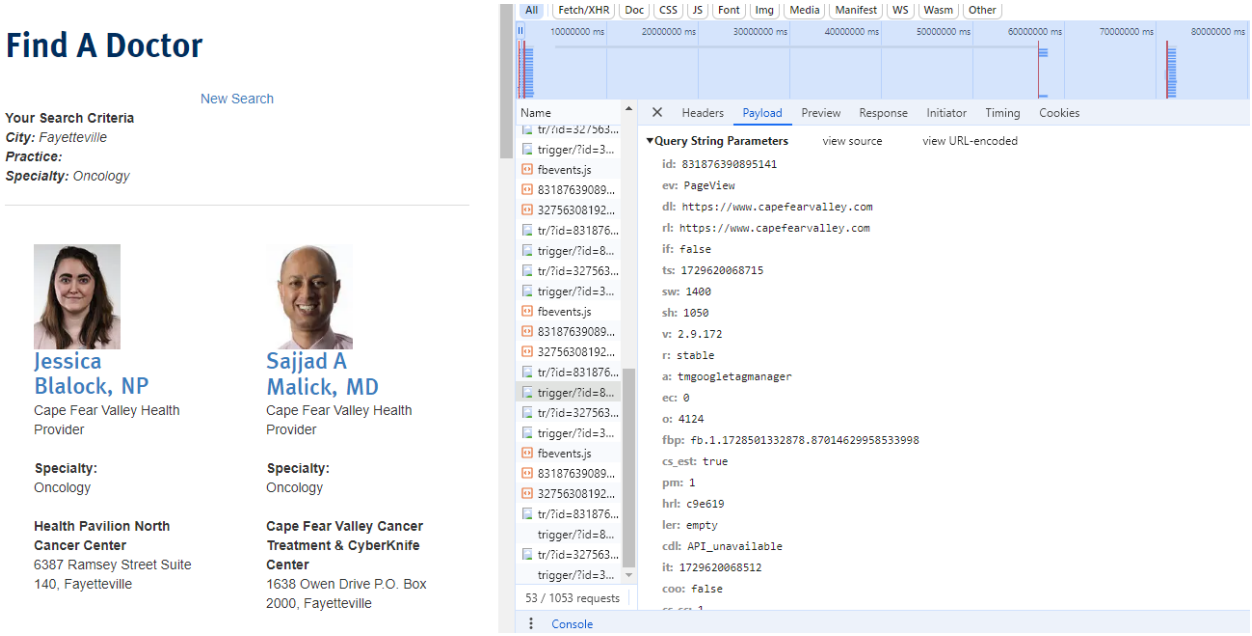


Figure 2: Depiction of a patient's search for a "Cancer (oncology)" provider on Cape Fear's Website being disclosed to Meta via a 'PageView' event.

Physician

New Search | Print Friendly View

Kenneth Manning, MD

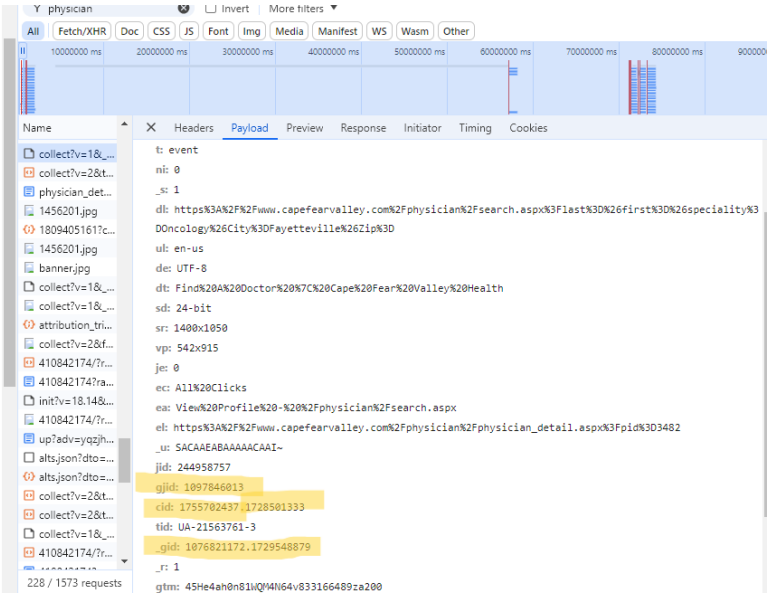
Cape Fear Valley Medical Center
Highsmith-Rainey Specialty Hospital

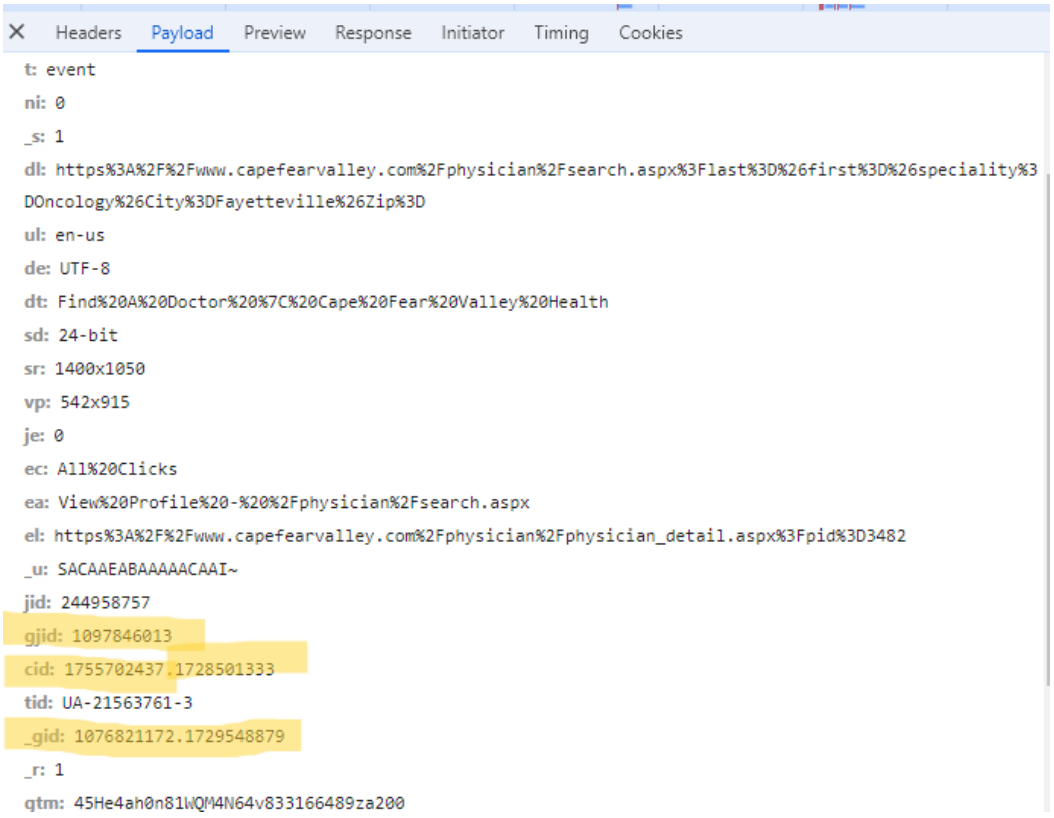
Oncology

Cape Fear Valley Cancer Treatment & CyberKnife Center
1638 Owen Drive
P.O. Box 2000
Fayetteville, NC 28304
Get Directions

Phone: (910) 615-6910
Fax: (910) 615-5626

Medical School: Medical College of Virginia, Richmond, VA
Residency: Wake Forest University/North Carolina Baptist Hospital, Winston-Salem, NC
Fellowship: Comprehensive Cancer Center of Wake Forest University, Winston-Salem, NC
Board Certification: American Board of Internal Medicine/Medical Oncology





Kenneth Manning, MD

Cape Fear Valley Medical Center
Highsmith-Rainey Specialty Hospital

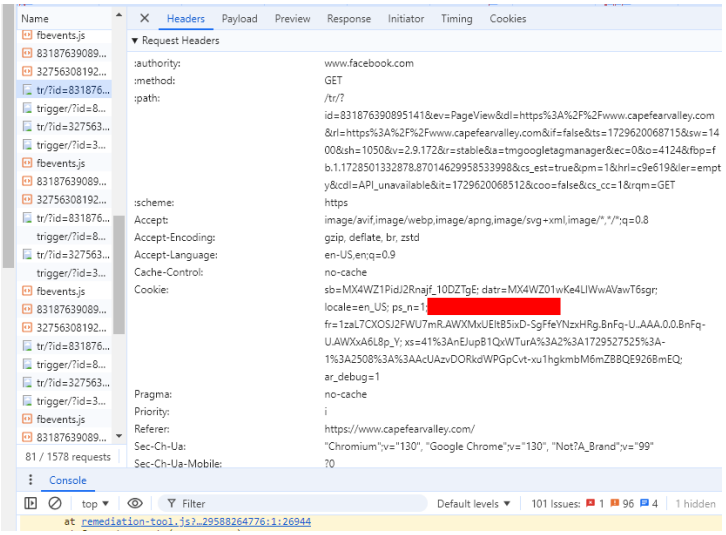
Oncology

Cape Fear Valley Cancer Treatment & CyberKnife Center
1638 Owen Drive
P.O. Box 2000
Fayetteville, NC 28304
Get Directions

Phone: (910) 615-6910
Fax: (910) 615-5626

Medical School: Medical College of Virginia, Richmond, VA
Residency: Wake Forest University/North Carolina Baptist Hospital, Winston-Salem, NC
Fellowship: Comprehensive Cancer Center of Wake Forest University, Winston-Salem, NC
Board Certification: American Board of Internal Medicine/Medical Oncology

Special Interests: Breast cancer, lung cancer, colon cancer, hematologic malignancies



Headers
Payload
Preview
Response
Initiator
Timing
Cookies
Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr/?
id=831876390895141&ev=PageView&dl=https%3A%2F%2Fwww.capefearvalley.com
&rl=https%3A%2F%2Fwww.capefearvalley.com&if=false&ts=1729620068715&sw=14
00&sh=1050&v=2.9.172&r=stable&a=tmgoogletagmanager&ec=0&o=4124&fbp=f
b.1.1728501332878.87014629958533998&cs_est=true&pm=1&hrl=c9e619&ler=empt
y&cdl=API_unavailable&it=1729620068512&coo=false&cs_cc=1&rqm=GET
:scheme: https
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Cookie: sb=MX4WZ1PidJ2Rnajf_10DZTgE; datr=MX4WZ01wKe4LIWwAVawT6sgr;
locale=en_US; ps_n=1;
fr=1zaL7CXOSJ2FWU7mR.AWXMxUEltB5ixD-SgFfeYNzxHRg.BnFq-U..AAA.0.0.BnFq-
U.AWXxA6L8p_Y; xs=41%3AnEJupB1QxWTurA%3A2%3A1729527525%3A-
1%3A2508%3A%3AAcUAzvDORkdWPGpCvt-xu1hgkmbM6mZ8BQE926BmEQ;
ar_debug=1
Pragma: no-cache
Priority: i
Referer: https://www.capefearvalley.com/
Sec-Ch-Ua: "Chromium";v="130", "Google Chrome";v="130", "Not?A_Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Filter
Default levels
101 Issues: 1 96 4
1 hidden
ion-tool.js?…29588264776:1:26944

Figures 3-4: Depiction of a patient's search and selection of a physician, with PHI and PII (including the gid, cid, c_user, datr, fr and the _fbp cookies) disclosed to Meta and Google by Cape Fear's installation and configuration of the Meta Pixel and Google Analytics.

86. Further, Cape Fear's Website captured disclosed patients' communications as they logged into and signed up for the patient portal, and patients' bill pay activities, see ***Figure 5*** below:

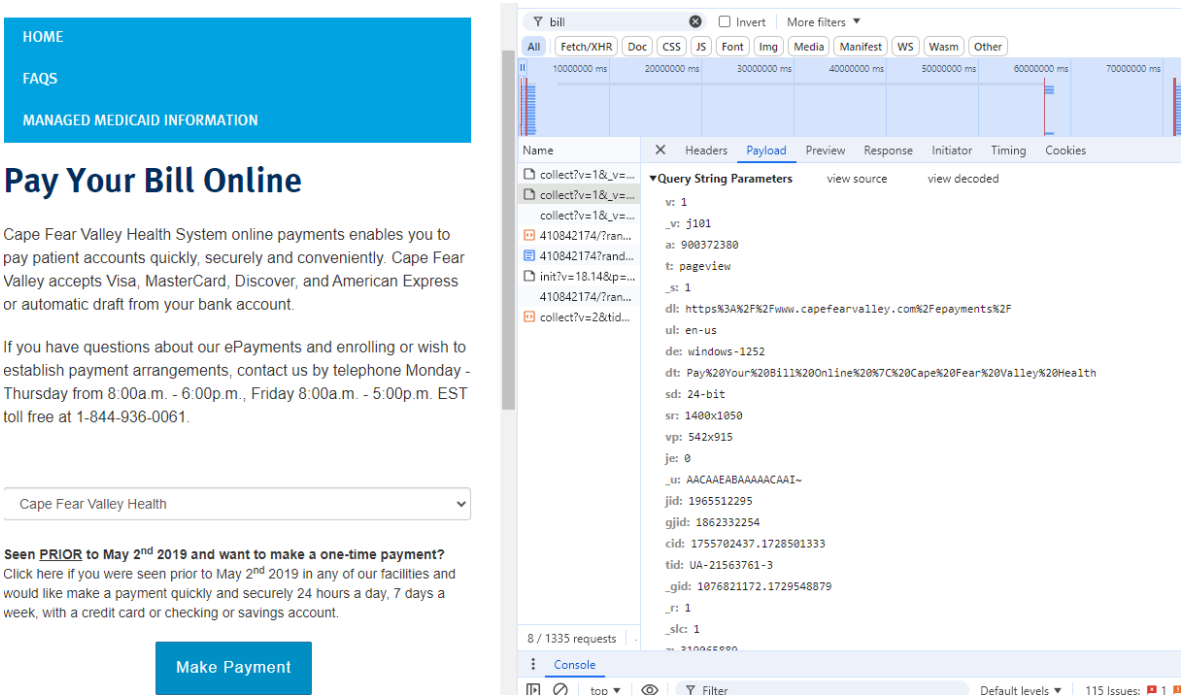


Figure 5: Depiction of Defendant capturing and disclosing patient's bill payment activities, with PHI and PII (including the _gid and cid cookies) disclosed by Cape Fear's Web Properties' Tracking Tools

87. In each of the examples above, the user's website activity and the contents of the user's communications are sent to Facebook and Google alongside their personally identifiable information. Several different methods allow marketers and third-parties to identify individual website users, but the examples above demonstrate what happens when the website user is logged into Facebook on their web browser or device. When this happens, the website user's identity is revealed via third-party cookies that work in conjunction with the Pixel. For example, the Pixel

transmits the user's c_user cookie, which contains that user's unencrypted Facebook ID, and allows Facebook to link the user's online communications and interactions to their individual Facebook profile.

88. Facebook receives several cookies when Cape Fear's Website transmits information via the Pixel, including the c_user, datr, and fr cookies, as evidenced by the images *supra*.

89. The "datr" cookie contains a unique alphanumeric code and identifies the specific web browser from which the user is sending the communication. It is an identifier that is unique to the user's web browser and is therefore a means of identification for Meta. Meta keeps a record of every datr cookie identifier associated with each of its users.

90. The fr cookie, a unique combination of the c_user and datr cookies, contains an encrypted Facebook ID and browser identifier.[30] Facebook, at a minimum, uses the fr cookie to identify users, and this particular cookie can stay on a user's website browser for up to 90 days after the user has logged out of Facebook.[31]

91. The datr and fr cookies are commonly referred to as third-party cookies because they were "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook. Although Facebook created these cookies, Defendant is ultimately responsible for the manner in which individual website users were identified via these cookies, and Facebook would not have received this data but for Defendant's implementation and use of the Pixel throughout the Cape Fear Website.

---

[30] Data Protection Commissioner, *Facebook Ireland Ltd: Report of Re-Audit*, p. 33 (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf (last visited Aug. 30, 2024).

[31] *Cookies & other storage technologies*, https://www.facebook.com/policy/cookies/ (last visited Aug. 30, 2024).

92. Defendant also revealed the Website visitors' identities via first-party cookies such as the _fbp cookie that Facebook uses to identify a particular browser and a user, *see Figure 8:*

```
rl: https://www.capefearvalley.com
if: false
ts: 1733847145295
sw: 1920
sh: 1080
v: 2.9.178
r: stable
a: tmgoogletagmanager
ec: 0
o: 4124
fbp: fb.1.1733344629926.821875157966991060
```

93. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Cape Fear's use of the Facebook Meta Pixel program. The fbp cookie emanates from Defendant's Website as a putative first party cookie, but is transmitted to Facebook through cookie synching technology that hacks around the same-origin policy. Therefore, the _fbp cookie is transmitted to Facebook even when the user's browser is configured to block third-party tracking cookies.

94. The __ga and _gid cookies operate similarly as to Google.

95. The Facebook Pixel uses both first- and third-party cookies to link website visitors' communications and online activity with their corresponding Facebook profiles, and, because the Pixel is automatically programmed to transmit data via both first-party and third-party cookies, customers' information and identities are revealed to Facebook even when they have disabled third-party cookies within their web browsers.

96. At present, the full breadth of Cape Fear's tracking and data sharing practices is unclear, but other evidence suggests Defendant has been using additional Tracking Tools to transmit its patients' PHI and PII to additional third parties. For example, Plaintiff's counsels'

investigation revealed that Defendant is also sending their patients' protected health information to Google via Google tracking tools including Google Analytics and Google Tag Manager.

97. Google Tracking Tools installed on the Cape Fear Website appear to collect the same types and categories of sensitive PHI and PII from Defendant's patients as the Facebook Pixel.

Figure 9: Example of Cape Fear's Website sending information to Google that a patient is attempting to pay their bill.

98. As described *supra*, this information is shared with Google along with the CID, __ga and _gid cookies.

99. Based on the above examples of how the Tracking Tools operate on Cape Fear's Website, Meta and Google would know (i) that a particular individual—who Meta and Google could identify based on their respective accounts—was a patient or prospective patient of Cape Fear seeking healthcare services, (ii) that the named patient searched for information regarding

their specific medical condition (for example, cancer), and (iii) that the patient in question was attempting to make an appointment with specific physicians, pay their bill, or log into their patient portal.

100. Meta and Google would also know the named patient's location and IP address, among other identifiers associated with the patient's computer or cell phone.

101. Using this PHI and PII, technology companies can put the named patient into a Core or Custom Audience for purposes of targeted advertising by Cape Fear or any other company seeking to advertise its services or products to individuals that fit the named patient's profile.

102. Cape Fear, Meta, Google, and other third parties profit off of Plaintiff's and Class Members' PHI and PII without their knowledge, consent, or authorization.

103. Defendant deprived Plaintiff and Class Members of their privacy rights when it: (a) embedded and implemented the Tracking Tools, which surreptitiously intercepted, recorded, and disclosed Plaintiff's and other online patients' and prospective patients' confidential communications and private information; (b) disclosed patients' and prospective patients' protected information to Meta and Google—unauthorized third parties; and (c) failed to provide notice to or obtain the consent from Plaintiff and Class Members to share their PHI and PII with others.

E. Plaintiff's Representative Experiences.

Plaintiff Donna Blue

104. Plaintiff Donna Blue accessed and used Defendant's Website through her computer and mobile devices while located in North Carolina to receive healthcare services from Defendant and at Defendant's direction.

105. Plaintiff has been a patient of Defendant since approximately 2019 and used Defendant's Website to request and book doctor's appointments for herself as well as search for and communicate information related to her ongoing dialysis treatment, wellness checks, mental health treatment, and medications.

106. As a condition of receiving Defendant's services, Plaintiff Blue disclosed her Private Information to Defendant on numerous occasions, and most recently in August of 2024.

107. Plaintiff Blue has an active Facebook account and an active Google account during the time she was providing her PHI and PII to Defendant via its Website.

108. After she provided information to Defendant regarding her PHI and PII, Plaintiff Blue began receiving targeted advertisements on her Facebook and Instagram accounts, inviting her to visit other Cape Fear Valley Health locations, as well as advertisements related to mental health and dialysis treatments.

109. Plaintiff Blue reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by any third party without her full knowledge and informed consent.

110. Plaintiff Blue provided her PHI and PII to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

111. As described herein, Defendant worked along with Facebook to intercept Plaintiff Blue's communications, including those that contained confidential PHI and PII, while Plaintiff was within the state of North Carolina.

112. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent or express written authorization.

113. Within the State of North Carolina, Defendant transmitted Plaintiff's FID, unique Google identifiers, computer IP address, location, information such as medical treatments and conditions, the information on physician(s) she selected and her sensitive and private medical information to Facebook and Google.

114. The full scope of Defendant's interceptions and disclosures of Plaintiff's communications to third party data brokers can only be determined through formal discovery. However, Defendant intercepted at least communications about Plaintiff's past or present patient status, medical conditions, treatments sought including dialysis and mental health services, and the locations for receipt of healthcare, via descriptive long-URLs, microdata and the inner text of buttons clicked by Plaintiff on the Website, that were sent to Meta via the Pixel and which contained information concerning Plaintiff's specific medical conditions, queries, and treatments sought.

115. By doing so without her consent, Defendant breached Plaintiff's right to privacy and unlawfully disclosed her PHI and PII.

116. Defendant did not inform Plaintiff that it shared her PHI and PII with Facebook.

117. Plaintiff would not have utilized Defendant's medical services and/or used its Website or would have paid much less for Defendant's services had she known that her Private Information would be captured and disclosed to third parties like Facebook and Google without her consent.

118. Plaintiff suffered damages in, inter alia, the form of (i) invasion of privacy; (ii) violation of confidentiality of her PHI and PII; (iii) loss of benefit of the bargain; (iv) diminution of value of the PHI and PII; (v) statutory damages and (vi) the continued and ongoing risk to her PHI and PII.

119. Plaintiff has a continuing interest in ensuring that her PHI and PII is protected and safeguarded from future unauthorized disclosure. Plaintiff wants to continue to communicate through online platforms but has no practical way of knowing if her communications are being intercepted and disclosed to Facebook and/or Google, and thus continues to be at risk of harm from Defendant's conduct.

F. Cape Fear's Conduct Violates Its Own Privacy Policies and Promises.

120. Defendant's privacy policies represent to Plaintiff and Class Members that Defendant will keep PHI and PII private and confidential and Cape Fear will only disclose PHI under certain circumstances, none of which apply here.

121. Cape Fear's Privacy Policy explains Defendant's legal duties with respect to PHI and PII and the exceptions for when Defendant can lawfully use and disclose it.

122. Defendant's Joint Notice of Privacy Practices states that "We are required by law to maintain the privacy of protected health information, to notify you following a breach of your unsecured protected health information, and to give you this Joint Notice about our privacy practices that explains how, when and why we may create, receive, maintain or transmit your PHI."[32]

123. Defendant's Joint Notice of Privacy Practices further outlines how Defendant may use and disclose medical information for treatment, payment, healthcare operations, appointment reminders, health-related benefits and services, individuals involved in your care or payment for your care and special purposes when permitted or required by law.[33]

[32] *See* https://www.capefearvalley.com/patients/forms/NPPEnglish.pdf (last updated April 22, 2024).

[33] *Id.*

124. However, other uses of medical information not covered by the Joint Notice of Privacy Practices, such as marketing[34] and retargeting require written authorization.[35]

125. At no point did Defendant seek such authorization from Plaintiff before transmitting protected health information to a third party for marketing purposes.

126. Defendant violated its own Joint Notice of Privacy Practices by unlawfully disclosing Plaintiff's and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties without written authorization.

127. This language reflects Defendant's awareness of the high value patients such as Plaintiff and Class Members place on their protected health information.

128. Defendant's transmission of protected health information to third parties such as Facebook or Google violated its own Notice of Privacy Practices, in which Cape Fear acknowledges that "[w]e are required to follow the privacy practices described in this Joint Notice."[36]

129. Cape Fear's examples of how and where it collects PHI and PII do not include patients' searches for specific medical conditions, treatments, providers, appointment details, nor does Defendant disclose that it will collect PHI and PII and send it to third-party data brokers, such as Meta, for marketing purposes.[37]

---

[34] The only type of marketing covered by the Joint Notice of Privacy Practices (not requiring patient authorization) is marketing within the Cape Fear Health System itself: "We may use your PHI to identify a service which may be of benefit to you, or new services offered by CFVHS. If you do not want CFVHS to mail you marketing information, you must notify the Director of Marketing in writing. . . . ***CFVHS will not sell your PHI to a third party.***"

[35] *Id.*

[36] *Id.*

[37] *Id.*

130. Defendant's Privacy Policy does not permit Defendant to intercept, transmit, or disclose Plaintiff's and Class Members' PHI and PII to third parties, including Meta, for marketing purposes.[38]

131. Defendant violated its own privacy policies by unlawfully intercepting and disclosing Plaintiff's and Class Members' PHI and PII to Meta and other third parties without adequately disclosing that it shares such information with third parties and without acquiring the specific patients' consent or authorization to share it.

F. Exposure of PHI and PII Creates a Substantial Risk of Harm.

132. The FTC has recognized that consumer data is a lucrative and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[39]

133. The FTC also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (i) using industry tested and accepted methods; (ii) monitoring activity on networks to uncover unapproved activity; (iii)

[38] *Id.*

[39] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, at 2 (Dec. 7, 2009) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

verifying that privacy and security features function properly; and (iv) testing for common vulnerabilities or unauthorized disclosures.[40]

134. The FTC cautions businesses that failure to protect PHI and PII and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.[41] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

G. Plaintiff's and Class Members' PHI and PII is Valuable.

135. As many health care data industry experts have recognized, "[p]atients' medical data constitutes a cornerstone of the big data economy. A multi-billion dollar industry operates by collecting, merging, analyzing[,] and packaging patient data and selling it to the highest bidder."[42]

136. The personal, health, and financial information of Plaintiff and Class Members is valuable and has become a highly desirable commodity. One of the world's most valuable resources is the exchange of personal data.[43]

137. Defendant and vendors of the Tracking Tools that Defendant uses profit from their

---

[40] *Start With Security, A Guide for Business*, https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

[41] *See Taking Charge: What to Do if Your Identity is Stolen*, FTC, at 2 (2012), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf.

[42] Niam Yaraghi, *Who should profit from the sale of patient data?*, The Brookings Institution (Nov. 19, 2018), https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/.

[43] *The world's most valuable resource is no longer oil, but data* (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

use of Plaintiff's and Class member's personal data to target them with advertising and for other economic benefits, such as improving their internal operations.

138. The value of personal data is well understood and generally accepted as a form of currency. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[44] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[45] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

139. Business News Daily reported that businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., consumer satisfaction data) from consumers.[46] Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.[47]

140. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business's success. Research shows that organizations

[44] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[45] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[46] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)* (Aug. 5, 2022; updated May 30, 2023), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[47] *Id.*

who "leverage customer behavioral insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[48]

141. In 2013, the Organization for Economic Cooperation and Development ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[49] There, OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[50]

142. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[51]

143. Unlike financial information, such as credit card and bank account numbers, PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable.[52]

---

[48] Brad Brown, *et al.*, *Capturing value from your customer data* (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[49] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, No. 220, OECD PUBLISHING PARIS (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[50] *Id.* at 25.

[51] *Id.*

[52] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters (July 21, 2020), https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/.

144. Consumers place considerable value on their PHI and PII and the privacy of that information.

145. Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[53]

146. CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[54]

147. In The Age of Surveillance Capitalism, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[55] In essence, Professor Zuboff explains that revenue from Internet user data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a market for this data.

148. Professor Paul M. Schwartz noted in the Harvard Law Review:

> Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of

---

[53] *See* https://time.com/4588104/medical-data-industry/.

[54] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

[55] Shoshanna Zuboff, THE AGE OF SURVEILLANCE CAPITALISM 166 (2019).

consumer information.[56]

149. Likewise, in The Wall Street Journal, former fellow at the Open Society Institute (and current principal technologist at the ACLU) Christopher Soghoian noted:

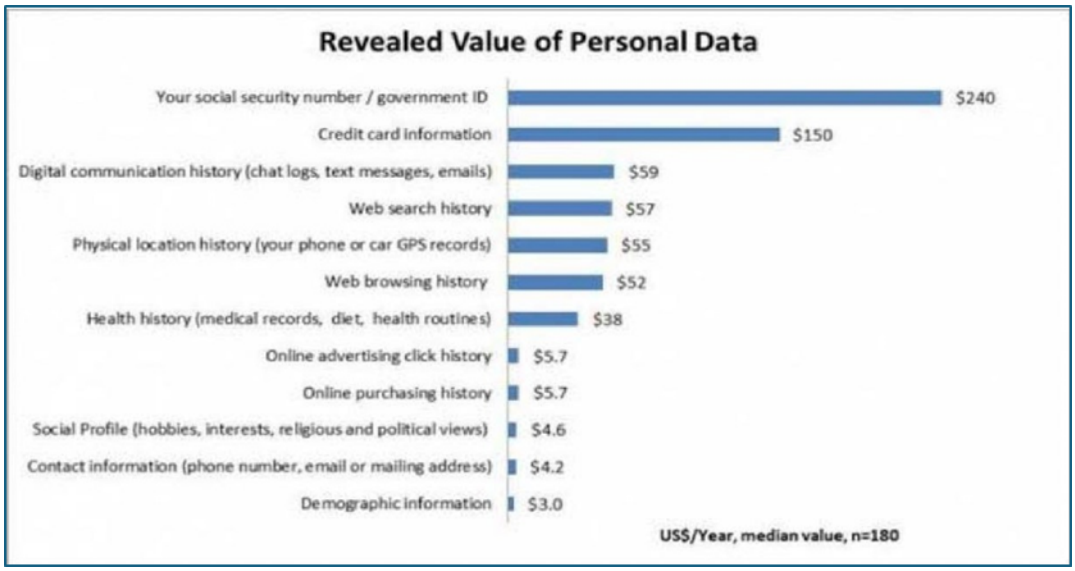
> The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data. Many of the major online advertising companies are not interested in the data that we knowingly and willingly share. Instead, these parasitic firms covertly track our web-browsing activities, search behavior and geolocation information. Once collected, this mountain of data is analyzed to build digital dossiers on millions of consumers, in some cases identifying us by name, gender, age as well as the medical conditions and political issues we have researched online. Although we now regularly trade our most private information for access to social-networking sites and free content, the terms of this exchange were never clearly communicated to consumers.[57]

150. The cash value of the personal user information unlawfully collected by Defendant provided during the Class Period can be quantified. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure.[58] Web browsing histories were valued at $52.00 per year.

[56] Paul M. Schwartz, Property, *Privacy and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (2004).

[57] Julia Angwin, How Much Should People Worry About the Loss of Online Privacy?, THE WALL STREET JOURNAL (Nov. 15, 2011).

[58] Tim Morey, What's Your Personal Data Worth?, DESIGN MIND (Jan. 18, 2011), https://web.archive.org/web/20131206000037/http://designmind.frogdesign.com/blog/what039sour-personal-data-worth.html.



151. Similarly, the value of user-correlated internet browsing history can be quantified, because Google Inc. was willing to pay users for similar information. Google had a panel called "Google Screenwise Trends" which, according to the internet giant, is designed "to learn more about how everyday people use the Internet." Upon becoming a panelist, internet users would add a browser extension that shares with Google the sites they visit and how they use them. The panelists consented to Google tracking such information for three months in exchange for one of a number of "gifts," including gift cards to retailers such as Barnes & Noble, Walmart, and Overstock.com. After three months, Google also agreed to pay panelists additional gift cards "for staying with" the panel. These gift cards, mostly valued at exactly $5, demonstrated that internet industry participants understood the enormous value in internet users' browsing habits. Google pays Screenwise panelists up to $3 per week to be tracked.

152. User-correlated URLs have monetary value. They also have non-monetary, privacy value. For example, in a study by the Pew Research Center, 93% of Americans said it was "important" for them to be "in control of who can get information" about them. Seventy-four percent said it was "very important." Eighty-seven percent of Americans said it was "important" for them not to have someone watch or listen to them without their permission. Sixty-seven

percent said it was "very important." And 90% of Americans said it was "important" that they be able to "control[] what information is collected about [them]." Sixty-five percent said it was very important.

153. Marketing services and consultants offering advice to companies on how to build their email and mobile phone lists—including those seeking to take advantage of targeted marketing—direct putative advertisers to offer consumers something of value in exchange for their personal information. "No one is giving away their email address for free. Be prepared to offer a book, guide, webinar, course or something else valuable."[59]

154. Several companies have products through which they pay consumers for a license to track their data. For example, Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect pay for browsing historical information.

155. Facebook also has paid users for their digital information, including browsing history. Until 2019, Facebook ran a "Facebook Research" app through which it paid $20 a month for a license to collect browsing history information and other communications from consumers between the ages of 13 and 35.

156. As Professors Acquisti, Taylor, and Wagman relayed in their 2016 article "The Economics of Privacy," published in the Journal of Economic Literature: "Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide

[59] VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER https://www.getvero.com/resources/twitter-lead-generation-cards/.

relevant advertising, or be traded with other parties."[60]

157.

158. Additionally, healthcare data is extremely valuable to bad actors. Health care records may be valued at up to $250 per record on the black market.[61]

159. Defendant's privacy violations exposed a variety of PHI including patient status, health conditions and symptoms, physicians, and other highly sensitive data.

160. PHI, like that exposed here, is likely even more valuable than Social Security numbers and just as capable of being misused.[62] PHI can be ten times more valuable than credit card information.[63] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, prescriptions, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, Social Security numbers.[64]

---

[60] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. OF ECON. LITERATURE 2, at 444 (June 2016). https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf

[61] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, *SecureLink* (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[62] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=(U)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market.

[63] Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[64] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

161. Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the $3 trillion healthcare sector.[65] "Rapid digitization of health records . . . have positioned hospitals as a primary arbiter of how much sensitive data is shared."[66]

162. The United States Supreme Court has explained that, "Confidential business information has long been recognized as property." *Carpenter v. United States*, 484 U.S. 19, 26 (1987). "Depriv[ation] of [the] right to exclusive use of … information" causes a loss of property "for exclusivity is an important aspect of confidential business information and most private property for that matter." *Id*. at 27. There is no doubt that Defendant has a "property right" in patients' data such that, if Facebook or Google took such information from Defendant without authorization, Defendant would have a claim for Facebook's or Google's taking of their property. Patients also have a property right in their own health information that may not be taken or used by Defendant without their authorization for non-health care related reasons.

H. Plaintiff and Class Members had a Reasonable Expectation of Privacy in their Interactions with Defendant's Web Properties.

163. Consumers assume the data they provide to hospitals will be kept secure and private.

164. In a survey related to Internet user expectations, most website visitors indicated that their detailed interactions with a website should only be used by the website and not be shared

[65] Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records* (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.

[66] *Id.*

with a party they know nothing about.[67] Website visitors expect that their interactions with a website should not be released to third parties unless explicitly stated.[68]

165. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its' customers' data.[69] A March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.[70] The same poll found that 63 percent of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.[71] A July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking computer use was an invasion of privacy.[72]

166. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of the iPhone operating software—which asks users for clear,

[67] *See Privacy and Online Tracking Perceptions Survey Report* (March 2020), CUJOAI, at 15–19, Privacy Survey_03-24 (cujo.com) (indicating major concerns of survey respondents was illegal use of data and unethical tracking and indicating respondents' belief that responsibility allocation falls on websites, and Internet users should be able to turn to the websites themselves, for privacy breaches).

[68] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).

[69] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.

[70] *Id.*

[71] *Id.*

[72] *Id.*

affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[73]

167. Like the greater population, Defendant's patients and prospective patients would expect the highly sensitive medical information they provided to Defendant through the Website to be kept secure and private.

I. Defendant's Conduct Violates HIPAA.

168. Under HIPAA, individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The [Privacy] Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.[74]

169. HIPAA "is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[75] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

170. HIPAA defines PHI as "individually identifiable health information" that is "created or received by a health care provider" (or similar entities) that "[r]elates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an

---

[73] Margaret Taylor, *How Apple screwed Facebook* (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[74] *Summary of the HIPAA Privacy Rule* (Oct. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[75] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103.

171. Identifiers such as patient-status (i.e., information that connects a particular user to a particular health care provider), medical conditions, health symptoms, treatments, and physicians, gathered in this case by the Tracking Tools through Cape Fear's Website, constitute protected health information.

172. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect.

173. When a regulated entity, like Defendant, collects the individual's information, that information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health, health care, or payment for care.

174. When Plaintiff communicated with Cape Fear regarding "treatment options" and other health-related information on the Cape Fear Website, the Tracking Tools intercepted and disclosed those communications to Meta and Google in violation of HIPAA's Privacy Rule.

CLASS ACTION ALLEGATIONS

175. Plaintiff brings this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and all others similar situated,

176. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the United States whose PHI and PII was disclosed to a third party through Defendant's Web Properties without authorization or consent during the applicable statute of limitations period.

177. The North Carolina Sub-Class that Plaintiff seeks to represent is defined as follows:

> All individuals residing in the State of North Carolina whose PHI and PII was disclosed to a third party through Defendant's Web Properties without authorization or consent during the applicable statute of limitations period.

178. The Nationwide Class and North Carolina Sub-Class are collectively referred to as the Class.

179. **The following people are excluded from the Class:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors and any entity in which Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's and Defendant's counsel and (6) the legal representatives, successors and assigns of any such excluded persons.

180. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Class to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues.

181. All members of the proposed Class are readily identifiable through Defendant's records.

182. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and 23(b)(3) are satisfied.

183. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Classes include tens of thousands of people based on Cape Fear's reported patient visits per year. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

184. **Commonality and Predominance.** This action involves common questions of law and fact to Plaintiff and Class Members, which predominate over any questions only affecting individual Class Members. These common legal and factual questions include, without limitation:

a. Whether Plaintiff's and Class Members' private communications were intercepted, recorded, and disclosed;

b. Whether the interception, recording, and disclosure of Plaintiff's and Class Members' communications was consensual;

c. Whether Defendant owed Plaintiff and the other Class Members a duty to adequately protect their PHI and PII;

d. Whether Defendant owed Plaintiff and the other Class Members a duty to secure their PHI and PII from interception and disclosure via third-party tracking technologies;

e. Whether Defendant owed Plaintiff and the other Class Members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Classes;

f. Whether Defendant knew or should have known of the risk of disclosure of data through third-party tracking technologies;

g. Whether Defendant breached its duty to protect the PHI and PII of Plaintiff and the other Class Members;

h. Whether Defendant knew or should have known about the inadequacies of its privacy protection;

i. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Classes' PHI and PII from unauthorized disclosure;

j. Whether proper data security measures, policies, procedures, and protocols were enacted within Defendant's computer systems to safeguard and protect Plaintiff's and the Classes' PHI and PII from unauthorized disclosure;

k. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Classes' injuries;

l. Whether Plaintiff and Class Members had a reasonable expectation of privacy in their PHI and PII;

m. Whether Plaintiff and Class Members suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

n. Whether Plaintiff and Class Members are entitled to recover damages; and

o. Whether Plaintiff and Class Members are entitled to other appropriate remedies including injunctive relief.

185. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of themselves and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

186. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI and PII, like that of every other Class Member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar manner.

187. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class and has retained counsel experienced in complex consumer class action litigation and intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Classes.

188. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of Class Members in a single action will provide substantial benefits to all parties and to the Court. Absent a class action, individual patients like

Plaintiff would find the cost of litigating their claims prohibitively high and would have no effective remedy for monetary relief.

189. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant has acted or refused to act on grounds that apply generally to the Class, thereby making monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As Defendant continues to engage in the practices described herein, the risk of future harm to Plaintiff and the Class remains, making injunctive relief appropriate. The prosecution of separate actions by all affected individuals with injuries similar to Plaintiff's, even if possible, would create a substantial risk of (a) inconsistent or varying adjudications with respect to individual patients, which would establish potentially incompatible standards of conduct for Defendant, and/or (b) adjudications with respect to individual patients which would, as a practical matter, be dispositive of the interests of the other patients not parties to the adjudications, or which would substantially impair or impede the ability to protect the interests of the Class. Further, the claims of individual patients in the defined Class are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

TOLLING, CONCEALMENT & ESTOPPEL

190. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

191. Defendant secretly incorporated Tracking Tools into its Website, providing no indication to users that their data, including their PHI and PII, would be disclosed to unauthorized third parties.

192. Defendant had exclusive knowledge that its Tracking Tools were incorporated on its Website yet failed to disclose that fact to patients and prospective patients or inform them that

by interacting with its Web Properties Plaintiff's and Class Members' PHI and PII would be disclosed to third parties, such as Meta and Google.

193. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Tracking Tools on Defendant's Web Properties is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Meta or Google to intercept PHI and PII.

194. The earliest Plaintiff and Class Members could have known about Defendant's conduct was approximately in July 2024 when she discussed her use of the Web Properties with counsel, and was informed of the surreptitious tracking engaged in by Defendant. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiff that her health information is not and will not be disclosed to any third party.

195. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

LEGAL CLAIMS

COUNT I

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1)
(On Behalf of Plaintiff & the Nationwide Class)

196. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully set forth herein.

197. The ECPA protects against intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

198. The ECPA protects both sending and receipt of communications.

199. The ECPA further provides any person who:

> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.
>
> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Id. §§ 2511(1)(c) & (d).

200. The primary purpose of the ECPA is to protect the privacy and security of communications as technology evolves.

201. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

202. Section 2520 provides for $10,000 in statutory damages for violations of ECPA. *Id.* § 2520(c)(2)(B).

203. The ECPA defines "intercept[ion]" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

204. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

205. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id*. § 2510(12).

206. The transmissions of PII and PHI from Plaintiff and Class Members to Defendant through Defendant's Web Properties are "electronic communications" under the ECPA. *See id*. § 2510(12).

207. The PHI transmitted by Plaintiff and Class Members include, but are not limited to, information regarding patient status, past and current health conditions and symptoms, treatments and care options, physicians, location, and other sensitive information.

208. Furthermore, Defendant intercepted the "contents" of Plaintiff's communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. PII such as patients' IP addresses, Facebook IDs, browser fingerprints and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of information generated when patients requested or made appointments;

g. The precise text of patient communications about specific treatments;

h. The precise text of patient communications about scheduling appointments with medical providers;

i. The precise text of patient communications about billing and payment;

j. The precise text of specific buttons on Defendant's Website that patients click to exchange communications including Log-Ins, Registrations, Requests for Appointments, Search and other buttons;

k. The precise dates and times when patients visit Defendant's Web Properties;

l. Information that is a general summary or informs third parties of the subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment and other information.

209. For example, Defendant's interception of the fact that a patient views a webpage like: https://www.capefearvalley.com/epayments/

210. Additionally, through its use of the Tracking Tools, Defendant intercepted and disclosed the communications about patient status, health conditions and symptoms, and other PHI and PII Plaintiff searched for on Defendant's Web Properties. This information was, in turn, used by third parties, such as Meta and Google, to (i) place Plaintiff in specific health-related categories; and (ii) target Plaintiff with advertising associated with Plaintiff's particular health conditions. Defendant knowingly transmitted this data and did so for the purpose of financial gain.

211. "Electronic, mechanical or other device" means "any device or apparatus which can be used to intercept . . . electronic communication[s]." *Id.* § 2510(5).

212. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Cape Fear, Meta, and Google use to track Plaintiff's and Class Members' communications;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing devices

d. Defendant's web servers; and

e. The Meta Pixel and Tracking Tools deployed by Defendant to effectuate the sending and acquisition of patient communications.

213. By embedding and deploying the Tracking Tools on Defendant's Web Properties, Defendant intentionally violated the ECPA, through its interception, attempt at interception, and its procurement of third parties to intercept the electronic communications of Plaintiff and Class Members.

214. Defendant also intentionally used or attempted to use the contents of Plaintiff's and Class Members' electronic communications, knowing that the information was obtained through interception. Defendant's use of the intercepted information and data for its own advertising and data analytics, in the absence of express written consent, violated ECPA.

215. Further, by embedding the Tracking Tools on its Web Properties and disclosing the content of patient communications relating to PHI and PII, without consent, Defendant had a purpose that was tortious, criminal, and designed to violate state and federal laws, including:

a. Negligence;

b. Breach of express contract;

c. Breach of implied contract;

d. Breach of fiduciary duty;

e. A violation of 42 U.S.C. § 1320d–6, the Administrative Simplification subtitle of HIPAA, which protects against the disclosure of individually identifiable health information to another person and is a criminal offense punishable by fine or imprisonment; and

f. A violation of HIPAA.

216. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3).

217. 42 U.S.C. § 1320d-6(a)(3) provides criminal and civil penalties against a healthcare provider who "knowingly . . . discloses individually identifiable health information to another person."

218. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual,* or the past, present, or future payment for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[76]

219. HIPAA prohibits disclosing patients' health information via tracking technologies. Defendant's use of the Tracking Tools violates HIPAA because the Meta Pixel and the other Tracking Tools transmit information that "identifies the individual" or, at a minimum, "there is a reasonable basis to believe that the information can be used to identify the individual," such as through unique identifying cookies and users' IP addresses.

[76] U.S.C. § 1320d(6) (emphasis added).

220. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed IIHI to Facebook without patient authorization.

221. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

222. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

223. As described above, Plaintiff entered data on Defendant's Web Properties relating to personal health conditions and other PHI, and later received targeted advertisements from Cape Fear. This shows that through the Tracking Tools employed, Defendant disclosed the IIHI of its Web Properties visitors to third parties in violation of the ECPA.

224. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in learning that:

a. Defendant intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about medical symptoms, conditions, medical appointments, healthcare providers and locations, medications and treatments and health insurance and medical bills) for commercial purposes has caused Plaintiff and Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' PII and PHI without providing any value or benefit to Plaintiff or Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' PII and PHI, such as understanding how people use its Web Properties and determining what ads people see on its Web Properties, without providing any value or benefit to Plaintiff or Class Members;

d. Defendant failed to provide Plaintiff and Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information and

e. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment and appointments that Plaintiff and Class Members intended to remain private no longer private.

225. Patients have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class Members' computing devices as "first-party" cookies that are not blocked.

226. Defendant's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below; and

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook.

227. At no time did Plaintiff or Class Members consent to Defendant's disclosure of their PHI and PII to Meta, Google, or other third parties. Plaintiff and the Class had a reasonable expectation that Defendant would not re-direct their communications content to Meta, Google, or others attached to their personal identifiers in the absence of their knowledge or consent.

228. Any purported consent that Defendant received was not valid.

229. Defendant has improperly profited from its invasion of Plaintiff's and Class Members' privacy in its use of their data for its economic value.

230. Defendant knew that such conduct would be highly offensive. Regardless, it proceeded to embed the Tracking Tools and use them to the detriment of visitors to its Web Properties.

231. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages and attorney's fees and costs.

COUNT II

BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiff & the Nationwide Class)

232. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

233. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

234. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiff first received medical care from Defendant.

235. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

236. Under these express contracts, Defendant and its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' PII/PHI: (i) provided to obtain such healthcare or (ii)

created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

237. Both the provision of medical services and the protection of Plaintiff and Class Members' Private Information were material aspects of these express contracts.

238. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiff and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Joint Notice of Privacy Practices.

239. At all relevant times, Defendant expressly represented in its Joint Notice of Privacy Practices, among other things that Defendant is "required to obtain [patient] written authorization for uses and disclosures other than for those purposes identified in the sections [of the Joint Notice], any disclosure of psychotherapy notes, disclosures of PHI for marketing purposes, or any sale of [patient] PHI."[77]

240. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

241. Consumers of healthcare value their privacy, the privacy of their dependents and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry

[77] Joint Notice of Privacy Practices, https://www.capefearvalley.com/patients/forms/NPPEnglish.pdf (last updated April 22, 2024).

standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

242. Plaintiff and Class Members would not have entered into these contracts with Defendant or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

243. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

244. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

245. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Google and Meta through the Google and Meta Collection Tools, including the Meta Pixel, Google Analytics and Google DoubleClick Ads on its Web Properties.

246. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Google and Meta through the Google and Meta Collection Tools, including the Meta Pixel, Google Analytics and Google DoubleClick Ads on its Web Properties.

247. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Google and Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

248. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of the bargain and instead received healthcare services that were of a diminished value.

249. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

250. Had Defendant disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, neither Plaintiff, Class Members nor any reasonable person would have purchased healthcare from Defendant or its affiliated healthcare providers.

251. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Google and Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses and the loss of the benefit of the bargain they struck with Defendant.

252. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Google and Meta.

COUNT III

BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff & the Nationwide Class)

253. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

254. Plaintiff and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

255. Specifically, Plaintiff and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiff and Class Members first received medical care from Defendant.

256. The valid and enforceable express contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's implied duty of good faith and fair dealing, particularly due to Defendant's special relationship with Plaintiff as her healthcare provider.

257. Under these express contracts, Defendant and its affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiff and Class Members. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

258. In service of its implied duty of good faith and fair dealing when executing the contract, Defendant was bound to not voluntarily divulge Plaintiff's and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

259. The express contracts for the provision of medical services are formed and embodied in multiple documents.

260. As evidence of Defendant's knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiff's expectations of Defendant to do the same, at all relevant times, Defendant expressly represented in its Privacy

Notice, among other things: that (i) "[w]e are required by law to maintain the privacy of protected health information, to notify you following a breach of your unsecured protected health information, and to give you this Joint Notice about our privacy practices that explains how, when and why we may create, receive, maintain or transmit your PHI;" and (ii) "[i]n some situations, North Carolina or federal law may provide additional protections for your PHI. Where state or federal law requires that we obtain your written consent before disclosing your PHI, we will do so."[78]

261. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, evidence Defendant's knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

262. Consumers of healthcare value their privacy, the privacy of their dependents and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

263. Plaintiff and Class Members would not have entered into these contracts with Defendant or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

[78] Joint Notice of Privacy Practices, https://www.capefearvalley.com/patients/forms/NPPEnglish.pdf (last updated April 22, 2024).

264. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and, through Defendant's implied duty of good faith and fair dealing, the protection of their Private Information.

265. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

266. Defendant did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Google and Meta through the Google and Meta Collection Tools, including the Meta Pixel, Google Analytics and Google DoubleClick Ads on its Web Properties.

267. Defendant breached its implied duty of good faith and fair dealing to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Google and Meta Collection Tools, including the Meta Pixel, Google Analytics and Google DoubleClick Ads on its Web Properties.

268. The mass and systematic disclosure of Plaintiff's and Class Members' Private Information to third parties, including Google and Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of its implied duty of good faith and fair dealing.

269. Due to Defendant's failure to fulfill the data privacy protections inherent in the special relationship with Plaintiff and the Class Members, and resulting breach of its implied duty of good faith and fair dealing, Plaintiff and Members of the Class did not receive the full benefit of the bargain and instead received healthcare and other services that were of a diminished value.

270. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

271. Had Defendant disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, neither Plaintiff, Class Members nor any reasonable person would have purchased healthcare from Defendant or its affiliated healthcare providers.

272. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' Private Information to Google and Meta, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses and the loss of the benefit of the bargain they had struck with Defendant.

273. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiff's and Class Members' Private Information to Google and Meta.

COUNT IV

BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiff & the Nationwide Class*)

274. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

275. As a condition of utilizing Defendant's Web Properties and receiving services from Defendant's healthcare facilities and professionals, Plaintiff and Class Members provided their PHI and PII and compensation for their medical care.

276. When Plaintiff and Class Members provided their PHI and PII to Defendant, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their PHI and PII without consent.

277. Plaintiff and Class Members would not have entrusted Defendant with their PHI and PII in the absence of an implied contract between them and Defendant obligating Defendant to not disclose PHI and PII without consent.

278. The valid and enforceable contracts to provide medical and health care services that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, PHI and PII given to Defendant or that Defendant gathers on their own from disclosure.

279. Both the provision of medical services and the protection of Plaintiff and Class Members' PHI and PII were material aspects of these contracts.

280. Plaintiff and Class Members would not have retained Defendant to provide healthcare services in the absence of an implied contract between them and Defendant obligating Defendant to not disclose PHI and PII without consent.

281. A meeting of the minds occurred, as Plaintiff and Class Members agreed to and did provide their PHI and PII to Defendant and paid for the provided healthcare in exchange for, amongst other things, the provision of healthcare and medical services and the protection of their PHI and PII.

282. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their PHI and PII.

283. Defendant breached these implied contracts by disclosing Plaintiff's and Class Members' PHI and PII without consent to third parties like Meta and Google.

284. Defendant materially breached the terms of these contracts including, but not limited to, the terms stated in the relevant Privacy Policy. Defendant did not maintain the privacy of Plaintiff's and Class Members' PHI and PII as evidenced by Defendant's sharing of that information with third parties such as Meta.

285. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

286. Had Defendant disclosed that its data privacy was inadequate or that it did not adhere to industry-standard privacy measures, Plaintiff and Class Members would not have purchased healthcare from Defendant.

287. As a direct and proximate result of the disclosure of Plaintiff's and Class Members' PHI and PII to Google and Meta, Plaintiff and Class Members have been harmed and have suffered actual damages and injuries including without limitation the release and disclosure of their PHI and PII, the loss of control and diminution in value of their PHI and PII, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

288. Plaintiff and Class Members are entitled to compensatory and consequential damages as a result of Defendant's breach of implied contract.

COUNT V

NEGLIGENCE
(On behalf of Plaintiff & the Nationwide Class)

289. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

290. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare services.

291. Upon accepting, storing and controlling the Private Information of Plaintiff and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

292. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due to the special relationship between Defendant and its patients, which is recognized by statute, regulations and common law.

293. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

294. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

295. Some or all of the healthcare, medical, or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

296. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

297. Defendant's duty to use reasonable care in protecting confidential data arose also because Defendant is bound by industry standards to protect confidential Private Information.

298. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

299. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Private Information through its use of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook and Google, gaining access to such Private Information for no lawful purpose.

300. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information.

301. Defendant's misconduct included the failure to (i) secure Plaintiff's and Class Members' Private Information; (ii) comply with industry standard data security practices; (iii) implement adequate website and event monitoring; (iv) implement systems, policies and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixel, Google Analytics, Google DoubleClick Ads and other tracking technologies and (v) prevent unauthorized access to Plaintiff's and Class Members' Private Information by sharing that

information with Google, Meta and other third parties. Defendant's failures and breaches of these duties constituted negligence.

302. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiff's and Class members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

303. Defendant's wrongful actions and inactions and the resulting unauthorized disclosure of Plaintiff's and Class members' Private Information constituted (and continue to constitute) negligence under common law.

304. Plaintiff and Class Members are entitled to compensatory, nominal and punitive damages, and Plaintiff and Class Members are entitled to recover those damages in an amount to be determined at trial.

305. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiff's and Class Members' Private Information with Google, Meta and other third parties without Plaintiff's and Class Members' express consent; and (iii) submit to future annual audits of its security systems and privacy monitoring procedures.

COUNT VI

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff & the Nationwide Class)

306. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

307. In light of the special physician-patient relationship between Defendant and Plaintiff and Class Members, which was created for the purpose of Defendant providing healthcare to Plaintiff and Class Members, Defendant became guardian of Plaintiff's and Class Members' Private Information. Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

308. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients and former patients, in particular, to keep secure their Private Information.

309. Defendant breached its fiduciary duties to Plaintiff and Class Members by disclosing their Private Information to unauthorized third parties, including Google and Meta, and separately, by failing to notify Plaintiff and Class Members of this fact.

310. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal and punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT VII

UNJUST ENRICHMENT
(On Behalf of Plaintiff & the Nationwide Class)

311. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein, except for the paragraphs specifically regarding breach of contract.

312. Plaintiff pleads this claim in the alternative to her breach of contract claim.

313. Plaintiff and Class Members conferred a benefit upon Defendant in the form of PHI and PII that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

314. Defendant benefits from the use of Plaintiff's and Class Members' PHI and PII and unjustly retained those benefits at their expense.

315. Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

316. The benefits that Defendant derived from Plaintiff and Class Members was not offered by Plaintiff and Class Members gratuitously and rightly belongs to Plaintiff and Class Members.

317. The services that Plaintiff and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide.

318. The medical services Defendant offers are available from other health care systems that protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiff's and Class Members' PHI and PII without consent, neither Plaintiff nor the Class Members would have purchased healthcare from Defendant.

319. By virtue of the unlawful, unfair, and deceptive conduct alleged herein, Defendant knowingly realized revenue from the use of Plaintiff's and Class Members' PHI and PII for profit by way of targeted advertising related to their respective medical conditions and treatments sought.

320. It would be inequitable under unjust enrichment principles in North Carolina and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

321. Plaintiff and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement and the imposition of a constructive trust to recover the amount of Defendant's ill-gotten gains and other sums as may be just and equitable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in her favor as follows:

A. Certification of the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

B. Designation of Plaintiff as representative of the Class and the undersigned counsel as Class Counsel;

C. That the Court enter an order:

1. Preventing Defendant from sharing Plaintiff's and Class Members' Private Information among other third parties;

2. Requiring Defendant to alert and otherwise notify all Users of its Web Properties of what information is being collected, used and shared;

3. Requiring Defendant to provide clear information regarding its practices concerning data collection from the Users/patients of Defendant's Web Properties, as well as uses of such data;

4. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and other third parties, and request Facebook/third parties to remove such information;

5. Requiring Defendant to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties;

6. Mandating the proper notice be sent to all affected individuals and posted publicly;

7. Requiring Defendant to delete, destroy and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution and disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and criminal asset recovery;

F. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

H. Plaintiff and the Class be awarded with treble and punitive damages insofar as they are allowed by applicable laws; and

I. Any and all other such relief as the Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Class, demand a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

Dated: December 11, 2024

/s/ David M. Wilkerson
David M. Wilkerson
N.C. Bar No. 35742
THE VAN WINKLE LAW FIRM
11 N Market Street
Asheville, NC 28801
Ph: (828) 258-2991
dwilkerson@vwlawfirm.com
Local Civil Rule 83.1(d) Counsel

Brandon M. Wise*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
IL Bar # 6319580*
One US Bank Plaza, Suite 1950
St. Louis, MO 63101
Ph: (314) 833-4825
bwise@peifferwolf.com

Andrew R. Tate*
PEIFFER WOLF CARR
KANE CONWAY & WISE, LLP
GA Bar # 518068*
235 Peachtree St. NE, Suite 400
Atlanta, GA 30303
Ph: 404-282-4806
atate@peifferwolf.com

David S. Almeida*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
T: (312) 576-3024
E: david@almeidalawgroup.com

**Pro Hac Vice applications to be submitted*

Attorneys for Plaintiff & the Putative Class